We claim:

- A method for operating a computer comprising:
 sensing whether a storage device has security information stored thereon;
 operating the computer in a full-access mode when the storage device has the
 device-specific security information; and
 operating the computer in a restricted-access mode when the storage device
 does not have the device-specific security information.
- 2. The method of claim 1, wherein operating the computer in a full-access mode includes the following:

encrypting digital data to be written to the storage disk; and decrypting digital data read from the storage device.

- 3. The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from format information for the storage device.
- 4. The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information etched on the storage device during manufacturing.
- 5. The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information specific to a removable media drive used for accessing the storage device.
- 6. The method of claim 5, wherein the drive-specific information includes a drive serial number.
- 7. The method of claim 5, wherein the drive-specific information includes

calibration parameters for the drive.

- 8. The method of claim 1 wherein operating the computer in a restricted-access mode includes operating the storage device in a read-only mode.
- 9. The method of claim 1, wherein operating the computer in a full-access mode includes permitting the user to access sensitive data stored on a remote computer.
- 10. The method of claim 1, wherein operating the computer in a full-access mode includes permitting the user to access a second storage device.
- 11. The method of claim 10, wherein operating the computer in a full-access mode includes decrypting digital data read from a second storage device using a cryptographic key generated from the device-specific security information.
- 12. The method of claim 1 wherein sensing the storage device is performed when a status change is detected for the storage device.
- 13. The method of claim 12, wherein the status change indicates the insertion of the storage device into the computer.
- 14. The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from security information written to the storage device during low-level formatting.
- 15. The method of claim 2, wherein the digital data is encrypted and decrypted using a cryptographic key generated from a unique identifier stored within an

electronic circuit embedded within the storage device.

16. A method for accessing a storage device comprising:

detecting a storage device within the storage drive;

sensing whether a storage device has security information stored thereon; and performing at least the following when the storage device has the device
specific security information:

encrypting digital data using the security information during a write access to write the digital data to the storage device; and decrypting digital data using the security information during a read access to read the digital data from the storage device.

- 17. The method of claim 16, wherein encrypting the digital data includes generating a cryptographic key as a function of format characteristics of an underlying storage medium of the storage device.
- 18. The method of claim 16, wherein encrypting the digital data includes generating a cryptographic key as a function of a unique identifier stored within an electronic circuit embedded within the storage device.
- 19. The method of claim 16 and further including preventing data from being written to the storage device during a write access when the storage device does not store the device-specific security information.
- 20. A method for accessing a storage device comprising: detecting a storage device within the storage drive; sensing whether a storage device has device-specific security information stored thereon; encrypting digital data using the device-specific security information when the

storage device has the device-specific security information; and writing the encrypted digital data to the storage device.

- 21. The method of claim 20, wherein encrypting digital data using the devicespecific security information generating a cryptographic key as a function of low-level format information for the storage device.
- 22. The method of claim 21, wherein encrypting digital data using the devicespecific security information includes generating a cryptographic key as a function of user-specific security information.
- The method of claim 22, wherein the user-specific security information is a password.
- 24. The method of claim 22, wherein the user-specific security information is biometric information.
- 25. The method of claim 24, wherein the biometic information is digital output from a retina scanner or a fingerprint scan.
- 26. The method of claim 21, wherein the format information includes a primary defect list.
- 27. The method of claim 21, wherein the format information includes one or more logical block addresses.
- 28. The method of claim 21, wherein generating the key includes computing an arithmetic sum of the format information.

- 29. The method of claim 21, wherein generating the key includes evaluating a polynomial using the format information as data for the polynomial.
- The method of claim 20, wherein writing the encrypted digital data includes writing the encrypted digital data to a removable storage medium.
- 31. The method of claim 30, wherein writing the encrypted digital data includes writing the encrypted digital data to a data storage diskette.
- 32. A method for securely accessing a storage device within a storage drive comprising:

 retrieving drive-specific information from the storage drive;

 generating a cryptographic key as a function of the drive-specific information;

 during a write access to the storage device, encrypting data using the cryptographic key and writing the encrypted data to the storage device via the storage drive; and during a read access to the storage device, reading encrypted data from the storage device and decrypting the data using the cryptographic key.
- 33. The method of claim 32, wherein the drive-specific information includes a drive serial number.
- 34. The method of claim 32, wherein the drive-specific information includes calibration parameters for the drive.
- 35. The method of claim 34, wherein the calibration parameters includes configuration parameters for read and write circuitry internal to the storage device.

- 36. The method of claim 35, wherein the calibration parameters are selected from the following set of calibration parameters for the storage drive: tracking parameters, a read channel boost, frequency cutoff values, read threshold values, alignment values, optical alignment correction factors and analog to digital conversion calibrations.
- 37. A method for securely accessing a plurality of storage devices within a storage drive comprising: retrieving format information from a first storage device; retrieving format information from a second storage device; and generating a cryptographic key as a function of the format information for the first storage device and the format information for the second storage device.
- 38. The method of claim 37, and further including:
 encrypting data using the cryptographic key during a write access to either
 the first storage device or the second storage device; and
 reading encrypted data and decrypting the read data using the cryptographic
 key during a read access to either the first storage device or the second
 storage device.
- 39. A method for operating a storage drive comprising:

 configuring the storage drive to operate in a read-only mode upon power-up;

 determining whether the storage device has device-specific security

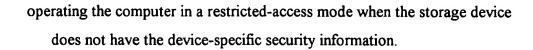
 information written thereon; and

 configuring the storage drive to operate in a read/write mode when the

 storage device within the storage drive has device-specific security

 information written thereon.

- 40. The method of claim 39 and further including configuring the storage drive to operate in a read-only mode when the storage device within the storage drive does not have device-specific security information written thereon.
- The method of claim 39 and further including preventing all read and write access to the storage device when the storage device within the storage drive does not have device-specific security information written thereon.
- 42. A computer-readable medium having computer-executable instructions for performing the method of:
 retrieving drive-specific information from a storage drive;
 generating a cryptographic key as a function of the drive-specific information;
 during a write access to the storage device, encrypting data using the
 cryptographic key and writing the encrypted data to the storage device
 via the storage drive; and
 during a read access to the storage device, reading encrypted data from the
 storage device and decrypting the data using the cryptographic key.
- 43. The computer-readable medium of claim 42, wherein the drive-specific information includes a drive serial number.
- 44. The computer-readable medium of claim 42, wherein the drive-specific information includes calibration parameters for the drive.
- 45. A computer-readable medium having computer-executable instructions for performing the method of:
 sensing whether a storage device has security information stored thereon;
 operating the computer in a full-access mode when the storage device has the device-specific security information; and

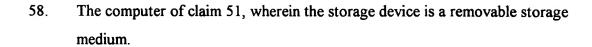


- The computer-readable medium of claim 45, wherein operating the computer in a full-access mode includes the following:

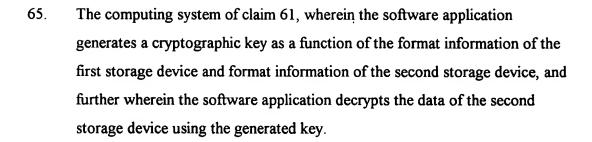
 encrypting digital data to be written to the storage disk; and decrypting digital data read from the storage device.
- 47. The computer-readable medium of claim 46, wherein the digital data is encrypted and decrypted using a cryptographic key generated from format information for the storage device.
- 48. The computer-readable medium of claim 46, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information etched into the storage device during manufacturing.
- 49. The computer-readable medium of claim 46, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information specific to a removable media drive used for accessing the storage device.
- 50. The computer-readable medium of claim 46, wherein the digital data is encrypted and decrypted using a cryptographic key generated from information specific to a user.
- 51. A computer comprising:
 - a drive for accessing a data storage device having security information stored thereon; and
 - a storage manager to selectively configure the computer to operate in a full-

access mode of operation or a restricted-access mode of operation as a function of the format information and security information stored on the storage device.

- 52. The computer of claim 51, wherein the storage manager generates a cryptographic key as a function of the security information and decrypts data stored on the storage device using the generated key.
- 53. The computer of claim 51, wherein the drive includes drive-specific information stored in a non-volatile memory, and further wherein the storage manager generates a cryptographic key as a function of the drive-specific information and decrypts data stored on the storage device using the generated key.
- 54. The computer of claim 51, wherein the storage device includes a serial number physically etched onto the storage device during manufacturing, and further wherein the storage manager generates a cryptographic key as a function of the serial number and decrypts data stored on the storage device using the generated key.
- 55. The computer of claim 51, wherein the storage manager generates a cryptographic key as a function of the format information and user-specific information and decrypts data on the storage device using the generated key.
- 56. The computer of claim 51, wherein the format information of the storage device includes a primary defect list.
- 57. The computer of claim 51, wherein the format information of the storage device includes one or more logical block addresses.



- 59. The computer of claim 51, wherein the storage device is a data storage diskette.
- The computer of claim 51, wherein the storage device has a disk-shaped storage medium.
- 61. A computing system comprising:
 - a first storage device having format information stored thereon;
 - a second storage device having data stored thereon; and
 - a software module executing within the computing system, wherein the software module selectively permits access to the data of the second storage device as a function of the format information and security information stored on the first storage device.
- 62. The computing system of claim 61, wherein the first storage device and second storage device are operatively coupled to two different computers that are communicatively coupled via a network.
- 63. The computing system of claim 61, wherein the first storage device and second storage device are operatively coupled to a single computer.
- 64. The computing system of claim 61, wherein the software application generates a cryptographic key as a function of the format information of the first storage device and decrypts the data of the second storage device using the generated key.



66. A computer comprising:

- a storage drive operating in a read-only mode upon power-up,
- a storage device operably coupled to the storage drive, wherein the storage device has security information stored thereon; and
- a storage manager to selectively configure the storage drive to operate in read/write mode as a function of the security information stored on the storage device.
- 67. The computer of claim 66, wherein the software application generates a cryptographic key as a function of the format information, verifies the security information on the storage device using the generated key and, upon verification, configures the storage drive to operate in read/write mode.